

MINUTES

Meeting number: 45

Venue: Rūnanga, Electricity Authority, Level 7, AON Centre, 1 Willis Street, Wellington

Time and date: 9.00am until 4.00 pm, Thursday 26 October 2023

Members Present

- Hon Heather Roy (Chair)
- Ben Gerritsen
- Barbara Elliston
- Chris Ewers
- Mike Underhill
- Nanette Moreau
- Paula Checketts
- Phil Gibson
- Allan Miller

Apologies

- Rebecca Larking

In attendance

Name	Title	Agenda item # attended
<u>Electricity Authority (Authority):</u>		
Andrew Millar	GM, Policy, Authority	#8-9 (until 11.40am)
Tim Sparks	Director of Network Pricing, Authority	#8f-13
Grant Benvenuti	Principal Advisor, Market Policy, Authority	All items excluding #3
James Blake-Palmer	Senior Analyst, Policy (Secretariat)	All items excluding #3
Peter Taylor	Manager Commercial, Authority	#8a, #8e, #10
Cheryl Eden	Commercial Contract Manager, MOSP (acting), Authority	#8e, #10
Will Goldsmith	Commercial Contract Manager, MOSP, Authority	#8d, #10
Chris Otton	Manager, Policy Operations, Authority	#6
	<u>Other:</u>	
Jonathon Berry	Principal Consultant, InPhySec	#8a-g, #9
Cobus Nel	GM Information Services and Technology, Transpower	#8b
Steve Smith	Security Services Manager, Transpower	#8b, via Teams
Tim Chadwick	Head of Energy Operations, NZX	#8c
Lyall McMillan	Head of Information Security, NZX	#8c

Name	Title	Agenda item # attended
Robbie Douglas	Chief Information Officer, NZX	#8c
Ian Hight	Client Director, Jade	#8d
Sam Johnstone	Head of Security, Jade	#8d
Greg Mathews	Senior Software Engineer, Jade	#8d, via Teams
Steve Foster	Infrastructure Architect, Jade	#8d, via Teams
Tim Aynsley	Head of Technology, Mercury NZ	#8f, via Teams
Jeff Whitty	Principal Advisor, Infrastructure Commission	#8g
John Clarke	Acting GM Operations, Transpower	#10
Richard Renouf	Compliance and Impartiality Manager, Transpower	#10
Lisa Tinkley	Business, Planning and Reporting Advisor, Transpower	#10

The meeting opened at 9.00am, James Blake-Palmer and Grant Benvenuti joined the meeting at 9.00am.

1. Attendance and apologies

- 1.1. The Chair welcomed members to the 45th meeting of the Security and Reliability Council (SRC). A quorum was established.
- 1.2. The Chair noted an apology from Rebecca Larking.

2. Changes to disclosure of interests

- 2.1. The Chair reviewed the interests register.
- 2.2. Barbara Elliston noted her *Unison Networks* directorship needs to be added.
- 2.3. There were no further changes disclosed. The Chair approved members to act despite those declared interests.

James Blake-Palmer and Grant Benvenuti left the meeting at 9.08am.

3. Members-only session

- 3.1. The members discussed their priorities for the meeting.

James Blake-Palmer and Grant Benvenuti joined the meeting at 9:28am.

4. Minutes of previous meeting

- 4.1. The minutes of the 1 June 2023 SRC meeting were discussed.
- 4.2. The minutes were accepted as a true and accurate record.

Mike Underhill moved. All members approved.

5. Correspondence

- 5.1. The Chair gave an overview of the correspondence including the letter sent to the Authority and the Authority's reply, noting members are given an opportunity to comment on drafts of letters of advice.
- 5.2. The Chair noted member views on the SRC's letter and the importance of clear meaning and moderate tone. The Chair asked members to give more of a steer to the secretariat with content and tone suggestions for both the draft letter and draft minutes.
- 5.3. Members discussed the issue of resilience and how that fits as part of the SRC's function. The secretariat outlined how resilience is described in the Code and the Electricity Industry Act 2010 (the Act).
- 5.4. The Chair, in discussions with the Board Chair and Chief Executive, will cover the SRC's understanding of the SRC's function, as described in the Act. The Chair will also discuss what the SRC has capacity for and its capacity for additional 'out of cycle' work.

6. Action list and updates

- 6.1. The Chair introduced this item and the secretariat ran through the list of completed actions. The Secretariat asked members to consider how they would like the information presented in this paper, to ensure it is useful and provides members with the right information at the right level of detail.
- 6.2. The Chair noted members' request for the secretariat to include in this paper information from other jurisdictions relevant to the meeting theme or to reliability and security of supply issues generally.
- 6.3. A member noted it would be good to receive updates from Authority staff on current work, relevant to winter 2023/24. The secretariat obtained the Chair's approval to invite an Authority representative to the meeting to provide information on current Authority workstreams relevant to this.

Chris Otton joined the meeting at 9.50am

Winter initiatives

- 6.4. Chris Otton noted an issues paper will be released in the next two weeks on *Standby Ancillary Services*. This will include a review and feedback on the 2023 initiatives in place.
- 6.5. Chris Otton also noted the Authority is placing emphasis on developing the emerging demand response market. Making the available demand response visible to the market system (scheduling, pricing and dispatch) ensures it is included in the calculation of peak demand.
- 6.6. A member noted, with regard to the possibility of a new grid-scale battery being made available to the market, this will not occur in time for Winter 2024.
- 6.7. Members noted the need for initiatives to be technology agnostic, to avoid counting things out and ensure aggregated resources enter the market. This requires the right information being made available to the market.

Action 1: The secretariat to add relevant items in the *Updates and Actions* paper from Authority staff on current workstreams for the February 2024 (Q1) meeting.

Action 2: The secretariat to include a standing Q4 item (in the *Actions and Updates* paper) covering developments/initiatives to manage forecast capacity issues for the coming winter and looking forward three years.

7. Risk radar (please see the latest version at the end of these minutes)

- 7.1. The Chair introduced this item and asked the secretariat to outline its approach to proposed layout and content changes for the risk radar.
- 7.2. The secretariat outlined the basis for the proposed changes. Member comments included:
 - a) A key, explaining time horizons and giving other navigation guidance, would be welcome
 - b) A proposal the secretariat include a 'traffic light' colour system to prioritise items in the risk radar and support its use as a mechanism to inform focus areas in the SRC's forward work programme
 - c) The radar could be grouped by 'effect' to help prioritise the SRC's focus on those issues most impactful.
 - d) There is no need for the previous style table as well as the new 'cause/effect' style table.

Action 3: The secretariat to liaise with the Chair on proposed risk radar changes and circulate for member input on both the proposed changes and member suggestions for the SRC's forward work programme.

Jonathon Berry and Andrew Millar joined at 10.10am

8. Technology and Information Security

- 8.1. The Chair welcomed Jonathon Berry to the meeting and introduced the Technology and Information Security theme.

InPhySec

- 8.2. Jonathon Berry gave a scene-setting presentation, which included the following points and discussion:
 - a) Criminals are monitoring data, seeking to take it hostage and extract maximum revenue by accessing and utilising the data, often using third parties.
 - b) The threat community is evolving faster than the protective community - timeframes to act are reducing, as data can be exploited within 24 hours of initial access.
 - c) Three key tenets apply to data – confidentiality, integrity and availability. Threat actors seek to disrupt these, especially targeting dated operational technology.
 - d) Physical and cyber-related attacks can have similar impacts, for example, both a 'terrorist attack' on an office and a DDOS cyber-attack on the systems can affect the ability of staff to supply their services
 - e) There is a potential need to consider paying a ransom to threat actors, depending on information as to how long attacks will impact.

- f) Quantum computing is increasingly being used by unconstrained threat actors against vulnerable equipment, such as significantly reducing the effectiveness of encryption systems
- g) Scenario-based sector-wide exercises are needed to test plans and responses to attacks on technology.
- h) There is no compulsion and little incentive to report attacks. This results in under-reporting and prevalence of privately paid ransoms with limited sharing of information for learning purposes
- i) Some countries may be less motivated to address cyber-threat issues, as it they may be a significant income stream, for example Nigerian email scams
- j) Insider threats are among the most dangerous, as there are often high levels of trust and deeper knowledge of an entity's vulnerabilities.
- k) Cyber-security should be seen as a risk like any other, and high-performing organisations are treating it as both a governance and operational issue.

Cobus Nel joined at 10.40am and Steve Smith joined at 10.45am

Transpower/Energy Market Services (EMS)

- 8.3. The Chair introduced Transpower/EMS presenters to the meeting.
- 8.4. The presentation and discussion included:
 - a) A security overview, noting a key focus on segregation between corporate and sanctum realms using firewalls and multi-factor authentication
 - b) Protection of systems from threats via the internet and physical assets is critical to system security, along with phishing and cyber education
 - c) Offshore protection aims to address issues and attacks before they reach New Zealand and impact at the country level
 - d) Support groups, such as the Control Systems Security Information Exchange (CSSIE) and the National Cyber Security Centre (NCSC) should be supported, as they offer benefits of informal engagement and have roles to distribute information on major events
 - e) One issue with information sharing is the lag, often caused by the need to verify reports and information before notices are sent
 - f) One of the biggest impacts of Cyclone Gabrielle was to telecommunications infrastructure, for example equipment on bridges that were damaged
 - g) The USA, through the department of Homeland Security, offer good learnings, for example through quarterly exercises and 'capture the flag' scenarios

- h) Discussion about the issues subcontractor Ventia experienced when it was attacked while trying to access historical data from an old and unpatched server. The immediate disabling of connection avoiding any compromise with Transpower. Learnings were applied to business continuity and response processes
- i) Information about the upcoming GridEx VII, which modifies the scenarios used by the Consortium for Electric Reliability Technology (CERT) and adapts them to the New Zealand environment. GridEx VII will include more information about the current state of the grid at various stages during the exercise and a greater focus on cyber impacts
- j) A suggestion it would be good for the sector participants to be able to assess themselves against a common set of standards.

Cobus Nel and Steve Smith left the meeting at 11.18am

Tim Chadwick, Lyall McMillan and Robbie Douglas joined the meeting at 11.20am

NZX

- 8.5. The Chair introduced the presenters from NZX, whose presentation was taken as read. The presentation and points of discussion included:
- a) The 2021 distributed denial of service (DDoS) attack was described as resulting in the equivalent of 160 hours of high-definition movies targeting NZX's servers every second
 - b) Operational systems were largely unaffected through use of private, non-internet connections. The main impact was on the securities market environment where 'clear and transparent' trading was impacted by an inability to publish securities market information
 - c) Response plans benefitted from regular testing, running of scenarios and intensive exercises. The Financial Markets Authority (FMA) used the opportunity to improve its processes and applying a banking approach to the NZX's processes
 - d) The NZX focuses on the key risk areas of People, Process and Technology, with most focus on the former and separate reporting for security vs cyber risks.

Andrew Millar left at 11.40am

Tim Chadwick, Lyall McMillan and Robbie Douglas left at 11.58am

Ian Hight, Sam Johnstone, Greg Mathews and Steve Foster joined at 11.59am

Jade

- 8.6. The Chair introduced the presenters from Jade, whose presentation was taken as read. The presentation and points of discussion included:
- a) Jade's focus on early intervention and use of dedicated test systems
 - b) A new approach being considered as part of a roadmap to support best practice

- c) An acknowledgment there can always be improvements, with a belief Jade meets the standards expected of it and strives to improve where possible
- d) There is a need to constantly monitor and consider change where needed, to meet the increasing sophistication of threat actors
- e) Advice to industry is to find ways to remove bias from threat analysis and run exercises at least annually. When looking at scenario testing, consider the benefits sought and build appropriate measures into the assessment.

Ian Hight, Sam Johnstone, Greg Mathews and Steve Foster left at 12.22pm

Peter Taylor joined at 12.23pm

Electricity Authority – MOSP monitoring

- 8.7. The Chair introduced the presenter from the Authority, whose presentation was taken as read. The presentation and points of discussion included:
- a) An outline of the Authority's framework and approach to monitoring of Market Operations Service Providers (MOSPs)
 - b) Reliance on external auditors, including a rotation of lead reviewers to minimise bias
 - c) Regular reviews and meetings enable early consideration and discussion of risks.
 - d) The Authority is tendering for all MOSP contracts (apart from the system operator) from 2027 and will likely engage external resource in the process
 - e) The industry exercises supported by the Authority have largely focused on shortfall events, but this will likely expand in future sessions, given feedback this is desirable.

Peter Taylor left at 12.45pm

The meeting broke for lunch at 12.45pm and reconvened at 1.23pm

Tim Aynsley joined at 1.24pm

Tim Sparks joined at 1.25pm

Case Study - Mercury Energy's cyber security journey

- 8.8. The Chair introduced the presenter from Mercury. The presentation and points of discussion included:
- a) Background and information about Mercury's cyber-security experience and learnings, focusing on its generation assets
 - b) How Mercury uses quarterly status updates at governance level, and the use of results to identify shortcomings and discuss how to uplift performance
 - c) The need to use a common framework to demystify complex material for a wider audience to best understand and make key decisions

from. Mercury used a PWC model as part of its approach to drive commonality across its systems

- d) How risk areas for breaches often include third parties and supply chains
- e) The benefits of going back to key purpose and core objectives to help decision-making around cyber preparedness
- f) A view there are potential timeliness issues with receiving information about threats and attacks from groups like CSSIE and the need for plain language and openness to sharing to maximise learnings
- g) Reflections on a 2–3-year journey on improving cyber commonality and understanding.

Tim Aynsley left at 1.50pm

Jeff Whitty joined at 1.50pm

Cyber-information sharing within New Zealand's electricity sector

- 8.9. The Chair introduced Jeff Whitty, whose presentation of his research was taken as read. The presentation and points of discussion included:
- a) A strong trust model drives collaboration and sharing of information but there is still a reluctance to share information about the impact of a breach or attack.
 - b) Multiple forums exist – electricity sector operators share cyber-related information through a large number of forums already. Each serves a different niche and the sector appears to be well catered for.
 - c) Differing views between large and small participants – Differences can be seen in their perception of cyber-risk and who they are willing to share information with. Smaller businesses demonstrate a willingness to collaborate, while larger businesses seem more inclined to work alone.
 - d) Weak relationships with Central Government – There are many benefits to participating in information-sharing forums, but strengthened relationships with Government isn't a reported experience.
 - e) Several barriers exist – The top three barriers that constrain information sharing are the concern of reputational risk, but also the risk of incurring liabilities or being subjected to punitive regulatory action. Neither breaching the NZ Privacy Act or anti-collusion provisions in the Commerce Act are seen as significant concerns.
 - f) Commerce Commission settings – The survey explored four barriers to making cyber-security investments. Whether fair or not, getting funding approved by the Commerce Commission is the biggest barrier voiced by respondents.
 - g) A survey on minimum standards may help highlight those participants unprepared and in need of support.

Jeff Whitty left at 2.20pm

9. Wrap up discussion on Technology and Information Security theme

- 9.1. The Chair led a wrap up session on the theme for this meeting.
- 9.2. At the Chair's request, Jonathon Berry provided a summary of his impressions from the day, which included:
 - a) the recent appointment of personnel to dedicated head of security roles suggests there are differing levels of maturity across the sector and there is a lack of risk visibility
 - b) The need for threats and information about them to be in common language and treated like any other risk
 - c) If standards are introduced, there is risk they will be interpreted differently, which provides an opportunity by potentially showing weaknesses for others to act on
 - d) Information-sharing is problematic; anonymous platforms for sharing could work but there's a need to test the information, making it difficult
 - e) Cost of security is a barrier for some, but needs to be offset against costs of recovery, which are not fully understood. Insurance rarely covers the full cost
 - f) Impact on the wider system of a breach or attack is often misunderstood or not factored. There's a need to think beyond the individual but gaining visibility of the bigger picture is difficult
 - g) The National Institute of Standards and Technology (NIST) cybersecurity framework provides a standard to draw on but is risk driven, rather than based on minimum levels. Cybersecurity should be considered as both a compliance and a risk question, not just risk.
 - h) If minimum levels were considered there may need to be both time and budget cycles needed before expectations of compliance.
- 9.3. Members discussed the *Technology and Information Security* theme papers and presentations and considered what advice to provide to the Authority

Jonathon Berry left at 2.45pm

John Clarke, Richard Renouf and Lisa Tinkley joined at 2.45pm

10. System operator self-review of performance

- 10.1. The Chair introduced this item and welcomed representatives from the system operator. The presentation and points of discussion included:
 - a) The system operator's positive work arising from or involving Cyclone Gabrielle and the winter initiatives
 - b) The welcome delivery of Real Time Pricing (RTP) and work on a system operator strategic plan
 - c) The system operator's focus on investment in people, including training and simulations

- d) The need for the system operator to receive accurate and timely information from participants about generation assets, outages and network health
- e) The need for the system operator to share quality information about the peaking challenges highlighted by the system operator notices, the New Zealand Generation Balance report, and consultant reports
- f) The suggestion the self-review should have included certain items such as any rulings panel decisions that were made during the report period (for example C-2022-002) and the things that did not go well such as the issues with the review of the Security of Supply Forecasting and Information Policy (SOSFIP). This is especially the case where issues span more than one review period, as they risk being missed by both reviews.
- g) A member suggested it would be positive for the report to include information about timeliness, internal performance metrics and other system operator Code obligations.

John Clarke, Richard Renouf and Lisa Tinkley left at 3.20pm

11.Wrap up discussion on system operator annual self-review

- 11.1. The Chair led a wrap up session on the system operator annual self-review.
- 11.2. Members raised the question of whether an external review ought to be undertaken of the system operator, to provide additional guidance to the SRC and the Authority on its performance. It was noted the Code requires an annual self-review but this does not prevent additional reviews, if desirable or necessary.
- 11.3. Members discussed the report and the Authority's indicative response and considered what advice to provide to the Authority.

12.The purpose and scope of next meeting's substantive papers.

- 12.1. The Chair introduced this item and sought member views on proposed papers for the SRC's Q1 2024 meeting.
- 12.2. Members noted they would like longer time for presentations and discussions which may mean fewer items at each meeting.
- 12.3. Members would like an update from the Future Security and Resilience (FSR) team at the Q1 meeting.
- 12.4. A member suggested including a 'futurist' paper for the Q1 meeting, to support the theme of innovation.
- 12.5. The Chair asked Barbara Elliston to put together a paper for the Q1 meeting on gaps in the SRC's forward work programme, or the sector's understanding of key security and reliability risks.

13.The SRC's Forward Work Programme

- 13.1. The Chair introduced this item and sought member views on proposed themes and papers for the SRC's 2024 meetings.

- 13.2. Members noted the need for further focus on Winter 2024, including an update on initiatives and the work of FSR.
- 13.3. The Chair asked the secretariat to review the risk radar and use the suggested ‘traffic light’ approach to assess priorities for future themes and papers. This is noted above as an action item for the secretariat.

The meeting ended at 4.00pm

Risk Radar – Cause and Effect (see key below for guidance)

Priority	Cause	Effect	Horizon	Comments
	Reduced gas supply	Reduced generation	P	
	Insufficient collaboration	Increased costs, reduces reliability	P	
	Government policy misaligned with industry objectives	Reduced investment and confidence & reduced water for hydro output	P	
	Increased small scale DG	Network congestion	P	
	Weather events	Increased outages	P	
	Inadequate AUFLS	Blackouts	P	
	Cyber attack	Damages system assets	P	The focus of Q4 2023
	Physical attack	Damaged system assets	P	
	Pandemic	Reduced workforce, restricted travel	P	
	Less live work	Increased outages	P	
	Social media	Personnel/asset attacks	P	
	Natural disaster	Damaged system assets	P	A resilience issue
	Delayed tree regulations	Increased outages	S	
	Regulator strategic priorities misaligned with industry objectives	Reduced investment and confidence	S	
	Commerce Commission regulations	Inhibits investment	S	
	Supply chain	Reduced goods/services	S	
	Dry Year	Increased prices and emissions & reduced market confidence and investment	S	
	Increased intermittency	Reduced capacity and flexibility at peaks	S	
	Poor extended reserve implementation	Increased blackouts	S	
	Fragmented government approach	Delays	S	
	Lack of thermal	Reduced capacity and flexibility	L	
	Demand increases outpace generation capacity increases	Causing outages	L	
	Inefficient market response	Insufficient generation	L	
	Early thermal exit	Reduced capacity and flexibility	L	
	Poor/unenforced standards	Reduced power quality	L	Through noncompliance
	Insufficient DER uptake	Network instability	L	
	Generation market misaligned with policy changes	Reduced capacity and flexibility	L	
	Ageing assets	Increased failures	L	
	Over-reliance on AI and automation	Reduced emergency human input	L	Inadequate response leading to outages
	Ageing/emigrating workforce	Reduced institutional knowledge and people available to plan, design and build	L	
	EV uptake	Undermined LV network stability	L	

	Stranded asset costs	Reduced network viability	L	
	Simultaneous asset replacement	Reduced asset availability	L	

Key	Symbol/colour	Meaning	Horizon	Meaning
	Red	High priority	P	Persistent risks – could happen any time
	Amber	Medium priority	S	Risks that can manifest anytime in approx. the next year
	Green	Lower priority	L	Risks that can manifest in approx. 1-5 years